A Risk Assessment Methodology (RAM) for Physical Security

Violence, vandalism, and terrorism are prevalent in the world today. Managers and decision-makers must have a reliable way of estimating risk to help them decide how much security is needed at their facility. A risk assessment methodology has been refined by Sandia National Laboratories to assess risk at various types of facilities including US Mints and federal dams. The methodology is based on the traditional risk equation:

Risk = P_A * (1 - P_E) * C,
P_A is the likelihood of adversary attack,
P_E is security system effectiveness,
1 - P_E is adversary success, and
C is consequence of loss to the attack.

The process begins with a characterization of the facility including identification of the undesired events and the respective critical assets. Guidance for defining a design basis threat is included, as well as for using the definition of the threat to estimate the likelihood of adversary attack at a specific facility. Relative values of consequence are estimated. Methods are also included for estimating the effectiveness of the security system against the adversary attack. Finally, risk is calculated. In the event that the value of risk is deemed to be unacceptable (too high), the methodology addresses a process for identifying and evaluating security system upgrades in order to reduce risk.

Risk assessment
Physical security
Vulnerability analysis
Security effectiveness
Consequence
Likelihood of attack

Note: Each critical infrastructure (CI) follows a RAM process developed specifically for that CI. This white paper provides a general discussion of the RAM approach and does not address the differences between the different RAMs.

Analysis Methodology

An analysis methodology has been used to assess the vulnerability of physical protection systems for facilities. Figure 1 describes the order and sequence of the seven basic steps of the methodology.

1. Facility Characterization

An initial step in security system analysis is to characterize the facility operating states and conditions. This step requires developing a thorough description of the facility itself (the location of the site boundary, building locations, floor plans, and access points). A description of the processes within the facility is also required, as well as identification of any existing physical protection features. This information can be obtained from several sources, including facility design blueprints, process descriptions, safety analysis reports, environmental impact statements, and site surveys.

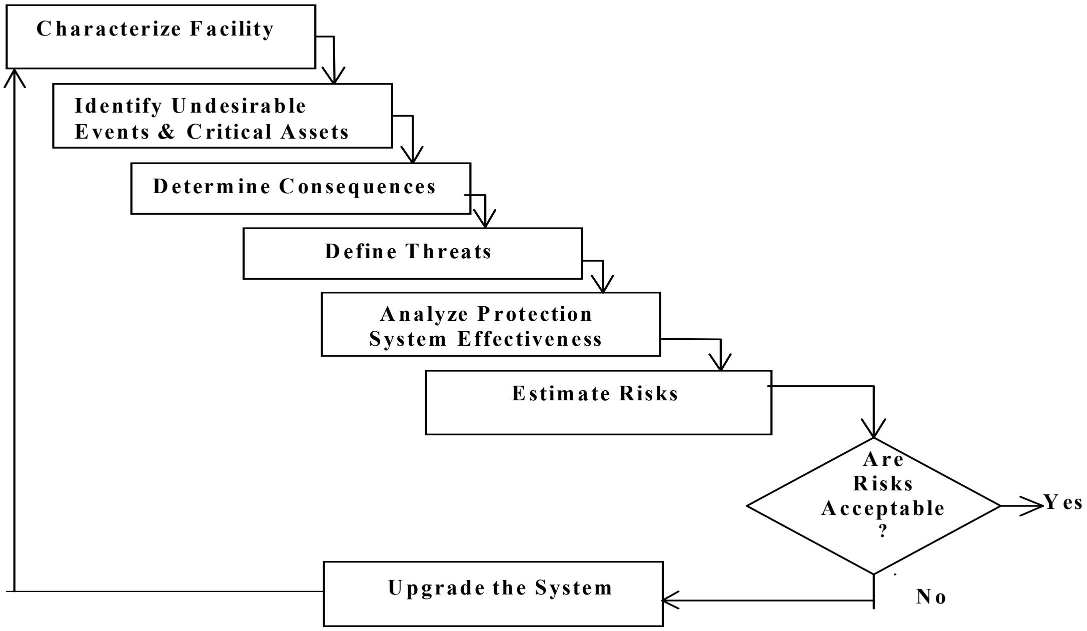


Figure 1. Steps in the Analysis Methodology

2. Undesired Events/Critical Assets Identification

Undesired Events- The undesired events must be established. Undesired events result in undesired consequences. Undesired events are site-specific and have adverse impacts on public health and safety, the environment, assets, mission, and publicity.

Critical Assets- The adversary could cause each undesired event to occur in several ways. A structured approach is needed to identify critical components for prevention of the undesired events. A logic model, like a fault tree, can be used to identify the critical components. The critical components and their locations become the critical assets to protect. Figure 2 is the top-level portion of a generic fault tree for facilities.

3. Consequence Determination

The next step is to categorize undesired events or loss of critical assets. The proposed categories of consequences are similar to those used by the Department of Defense per Military Standard 882C.

The consequence values and categories are described in Table 1. The goal is to estimate the relative consequence value associated with each undesired event.

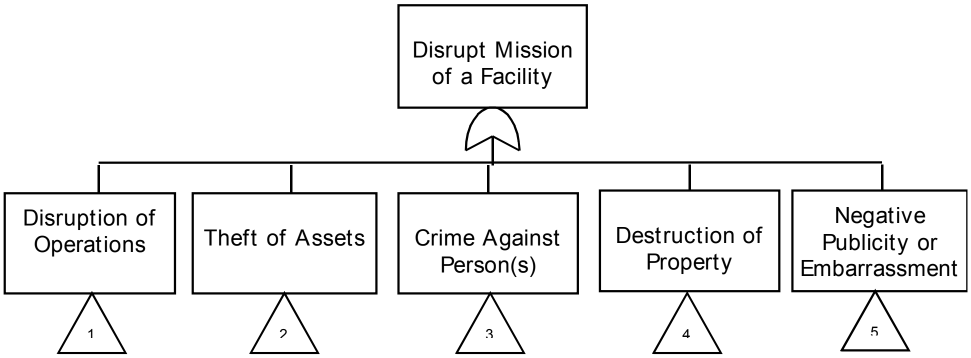


Figure 2. Top Level Generic Fault Tree

Table 1. Consequence Categories and Associated Values

Consequence Category	Consequence Value
Catastrophic-results in death(s), total mission loss, or severe environmental damage	Very high
Critical-results in severe injury/illness, major mission loss, or major environmental damage	High
Marginal-results in minor injury/illness, minor mission loss, or minor environmental damage	Medium
Negligible-results in less than minor injury/illness, less than minor mission loss, or less than minor environmental damage	Low

4. Threat Definition

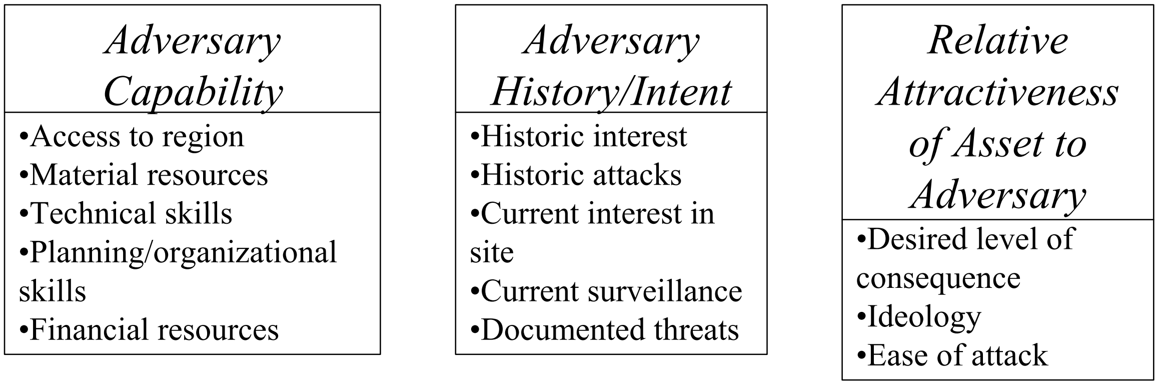
Threat- Before a vulnerability analysis can be completed, a description of the threat is required. This description includes the type of adversary, tactics, and capabilities (number in the group, weapons, equipment, and transportation mode). Also, information is needed about the threat to estimate the likelihood that they might attempt the undesired events. The specific type of threat to a facility is referred to as the design basis threat (DBT). The DBT is often reduced to several paragraphs that describe the number of adversaries, their modus operandi, the type of tools and weapons they would use, and the type of events or acts they are willing to commit.

The types of organizations that may be contacted during the development of a DBT description include local, state, and federal law enforcement (to include searching source material) and related intelligence agencies. Local authorities should be able to provide reports on the type of criminal activities that are occurring and analytical projections of future activities. A review of literature may be conducted to include past incident reports associated with the site, local periodicals, professional journals, and other related material.

Likelihood of Attack- After the threat spectrum has been described, the information can be used together with statistics of past events and site-specific perception to categorize threats in terms of likelihood that each type of threat would attempt an undesired event. Safety studies have historical data and statistics to predict the likelihood of an abnormal event and the system response to the event. For security studies, estimating the likelihood that an adversary group will attack a specific asset presents a challenge. Because of the human element – the fact that humans plan, rehearse, learn and modify in order to optimize the attack effectiveness, the events are not random and many of the required mathematical assumptions cannot be met. Human behavior is difficult to predict and providing a quantified prediction of human behavior is an even more difficult task.

The likelihood of adversary attack can be estimated with a qualitative relative threat potential parameter. Figure 3 describes the factors that can be used to estimate relative threat potential. The process for estimating the threat potential follows a complete threat analysis and the parameter is estimated per undesired event and per adversary group. The basis of the parameter estimation includes:

- Characteristics of the adversary group relative to the asset to be protected
- Relative attractiveness of the asset to the adversary group.



Adversary Capability

•Access to region
•Material resources
•Technical skills
•Planning/organizational skills
•Financial resources

Adversary History/Intent

•Historic interest
•Historic attacks
•Current interest in site
•Current surveillance
•Documented threats

Relative Attractiveness of Asset to Adversary

•Desired level of consequence
•Ideology
•Ease of attack

Figure 3. Estimating Likelihood of Attack, P_A

5. Protection System Effectiveness Analysis

Figure 4 describes the design and analysis process outline that can be used when estimating physical protection system effectiveness. The physical protection features must be described in detail before the security system effectiveness can be evaluated. An effective security system must be able to detect the adversary early and delay the adversary long enough for the security response force to arrive and neutralize the adversary before the mission is accomplished. In particular, an effective security system provides effective detection, delay, and response. These security system functions (detection, delay, and response) must be integrated to ensure that the adversary threat is neutralized before the mission is accomplished.

DETECTION, the first required function of a security system, is the discovery of adversary action and includes sensing covert or overt actions. In order to discover an adversary action, the following events must occur:

- sensor (equipment or personnel) reacts to an abnormal occurrence and initiates an alarm
- information from the sensor and assessment subsystems is reported and displayed
- someone assesses information and determines the alarm to be valid or invalid. (If determined to be a nuisance alarm (defined below), detection has not occurred.)

Methods of detection include a wide range of technologies and personnel. Entry control, a means of allowing entry of authorized personnel and detecting the attempted entry of unauthorized personnel and contraband, is included in the detection function of physical protection. Entry control, in that it includes locks, may also be considered a delay factor (after detection) in some cases. Searching for metal (possible weapons or tools) and explosives (possible bombs or breaching charges) is required for high-security areas. This may be accomplished using metal detectors, x-ray (for packages), and explosive detectors. Security police or other personnel also can accomplish detection. Security police or other personnel can contribute to detection if they are trained in security concerns and have a means to alert the security force in the event of a problem. An effective assessment system provides two types of information associated with detection: (1) information about whether the alarm is a valid alarm or a nuisance alarm, and (2) details about the cause of the alarm, i.e., what, who, where, and how many. The effectiveness of the detection function is measured by the probability of sensing adversary action and the time required for reporting and assessing the alarm.

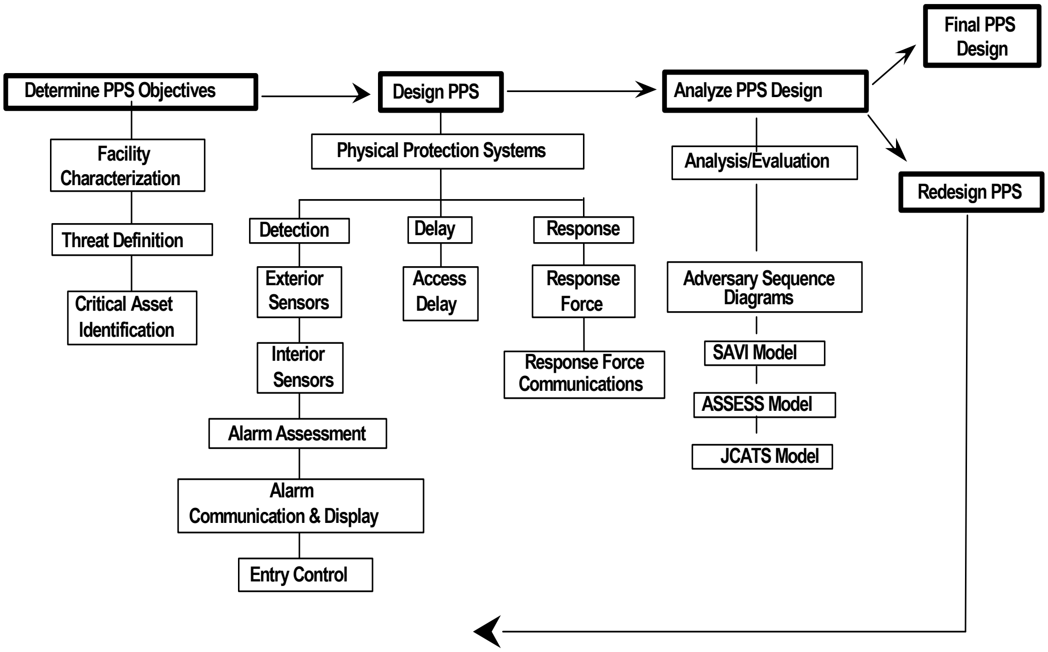


Figure 4. Design and Evaluation Process Outline (DEPO)

DELAY is the second required function of a security system. It impedes adversary progress. Delay can be accomplished by fixed or active barriers, (e.g., doors, vaults, locks) or by sensor-activated barriers, e.g., dispensed liquids, foams. The security police force can be considered an element of delay if personnel are in fixed and well-protected positions. The measure of delay effectiveness is the time required by the adversary (after detection) to bypass each delay element.

RESPONSE, the third requirement of security systems, comprises actions taken by the security police force (police force or law enforcement officers) to prevent adversarial success. Response consists of interruption and neutralization. The measure of response effectiveness is the time between receipt of a communication of adversarial actions and the interruption and neutralization of the action.

Interruption is defined as the response force arriving at the appropriate location to stop the adversary's progress. It includes the communication to the response force of accurate information about adversarial actions and the deployment of the response force. Neutralization is the act of stopping the adversary before the goal is accomplished. The effectiveness measures for neutralization are security police force equipment, training, tactics, and cover capabilities.

Protection System Effectiveness- Analysis and evaluation of the security system begin with a review and thorough understanding of the protection objectives and security environment. Analysis can be performed by simply checking for required features of a security system, such as intrusion detection, entry control, access delay, response communications, and a response force. However, a security system based on required features cannot be expected to lead to a high-performance system unless those features, when used together, are sufficient to ensure adequate levels of protection. More sophisticated analysis and evaluation techniques can be used to estimate the minimum performance levels achieved by a security system.

The Adversary Sequence Diagram (ASD) is a graphical representation of physical protection system elements along paths that adversaries can follow to accomplish their objective. For a specific physical protection system and threat, the most vulnerable path can be determined. This path with the least physical protection system effectiveness establishes the effectiveness of the total physical protection system. An ASD is developed for a single critical asset associated with an undesired event. Computer codes such as Systematic Analysis of Vulnerability to Intrusion (SAVI) and Analytic System and Software for Evaluating Safeguards and Security (ASSESS) can be used to determine the most vulnerable path. The neutralization module of ASSESS or Joint Combat and Tactical Simulation (JCATS) can be used to estimate response force effectiveness.

6. Risk Estimation

RISK- Risk is quantified by the following equation:

$$R = P_A * (1-P_E) * C$$

Where: R = risk associated with adversary attack
P_A = likelihood of the attack
P_E = likelihood that the security system is effective against the attack
$(1 – P_E)$ = likelihood that the adversary attack is successful (also the likelihood that security system is not effective against the attack)
C = consequence of the loss from the attack.

7. Upgrades and Impacts

System Upgrades- If the estimated risk for the threat spectrum is judged to be unacceptable, upgrades to the system may be considered. The first step is to review all assumptions that were made that affect risk. All assumptions concerning undesired events, target identification, consequence definition, threat description, estimation of likelihood of attack, and safeguards functions should be carefully reevaluated. Upgrades to the system might include retrofits, additional safeguard features, or additional safety mitigation features. The upgraded system can then be analyzed to calculate any changes in risk due to change in likelihood of attack, system effectiveness, or consequence values. If the estimated risk for the upgraded system is judged to be acceptable, the upgrade is completed. If the risk is still unacceptable, the upgrade process of assumption review and system improvement should be repeated until the risk is judged to be acceptable.

Upgrade Impact- Once the system upgrade has been determined, it is important to evaluate the impacts of the system upgrade on the mission of the facility and the cost. If system upgrades put a heavy burden on normal operation, a trade-off would have to be considered between risk and operations. Budget can be the driver in implementing security upgrades. A trade-off between risk and total cost may have to be considered. When balance is achieved in the level of risk and upgrade impact on cost, mission, and schedule, the upgraded system is ready for implementation. At this point, the design/analysis process is complete.

Methodology Summary

An analysis methodology for assessing the vulnerability of physical protection systems for facilities has been described. Vulnerability analyses for U.S. Mints and federal dams have been completed using the methodology. The methodology can be used to evaluate other important U.S. infrastructure components.

Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.